UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/745,863	12/21/2000	Howard Shelton Lambert	GB999141US1	2220

46369 7590 04/07/2005

HESLIN ROTHENBERG FARLEY & MESITI P.C.
5 COLUMBIA CIRCLE
ALBANY, NY 12203

EXAMINER	
ADAMS, JONATHAN R	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 04/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/745,863	LAMBERT ET AL.	
	Examiner	Art Unit	
	Jonathan R Adams	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 January 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

Applicant's arguments filed 01/27/2005 have been fully considered but they are not persuasive.

In response to applicant's argument that the sited reference does not teach sending a request from a decoding controller on the first data processing apparatus to a second data processing apparatus to determine attributes of a decoding process for accessing the encoded data, the examiner disagrees, '351 teaches the medium number 12 is loaded from the software storage medium 11. In step S14, the medium key is generated in the personal key generating circuit 211. The medium number is transferred to the user after the user requests the plaintext software (Col 7, Lines 15-23, '351).

In response to applicant's argument that the sited reference does not teach the elements of claim 4, the examiner disagrees. The Medium key (Col 1, Line 47, '351) can be defined as a cryptor or an authenticator based on the use provided in the claims. Further, an Internet search for the term "cryptor" yields definitions including cryptographic keys.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1, 4, 7, and 10-12 rejected under 35 U.S.C. 102(b) as being preceded by Hasebe et al., US Patent No 5392351 (hereafter referred to as '351).

3. As to claims 1 and 10-12:

'351 teaches a method for controlling access to data comprising:

- A requester requesting access to data stored in encoded form on a first data processing apparatus / User requests this plaintext (Col 7, Line 19, '351)
- Sending a request to a second data processing apparatus to determine attributes of a decoding process / Medium number is loaded from software storage medium to vendor computer (Col 7, Line 48, '351), (Fig 7a, '351), (Fig 3, '351)
- Receiving attributes at decoding controller on first data processing apparatus / software decrypting key is encrypted by the medium key so that the permission information is generated (Col 7, Line 57, '351) at vendor computer (Fig 3, '351). Permission information is sent to and stored on the software storage medium (Col 7, Line 57, '351).
- Performing the decoding process with determined attributes / Decrypting unit decrypts the encrypted electronic data based on the electronic data decrypting key and generates the plain text (Col 4, Line 27, '351)

4. As to claim 4:

Attributes include a cryptor used in encryption / Medium key (Col 1, Line 47, '351)

Cryptor required for decryption, electronic data decryption key based on the medium key (Col 1, Line 46, '351)

5. As to claim 7:

Attributes include one or more decoding keys for use in decryption or authentication / Medium key (Col 1, Line 47, '351)

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claim 2 rejected under 35 U.S.C. 103(a) as being unpatentable over '351 in view of "Security Service API".

As to claim 2:

8. '351 teaches a method for controlling access to data using encryption algorithms on a user computer. '351 does not teach for the user interaction to be conducted through an abstracting API. Security Service API teaches a general purpose cryptography API for use on user operated computers with the windows operating system whereby the cryptographic module details are abstracted (Chap 7.1, Line 1, "Security Service API"). It would have been obvious to a person of ordinary skill in the art at the time of invention to use the Windows based CryptoAPI as an abstraction layer

for the invention of '351. One of ordinary skill in the art would have been motivated to use the Windows based CryptoAPI as an abstraction layer for the invention of '351 because it is very common for computers to use the Windows operating system which relies on API's, such as the CryptoAPI for encryption.

9. Claim 3 rejected under 35 U.S.C. 103(a) as being unpatentable over '351 in view of Bruce Schneier, "Applied Cryptography"

As to claim 3:

10. '351 teaches a method for controlling access to data using encryption keys temporarily stored on an intermediary computer. '351 does not teach to store these keys in volatile memory and to delete the key at the end of the user session. Schneier teaches a secure key management strategy whereas a session key should be discarded after the communications session (Page 180, Line 4 et seq., Schneier). Schneier further teaches the simplifying advantage of not storing keys to disk from volatile system memory (Page 184, Line 13, Schneier). It would have been obvious to a person of ordinary skill in the art at the time of invention to use the key management techniques listed in Schneier with the encrypted communications of '351. One of ordinary skill in the art would have been motivated to use the key management techniques listed in Schneier with the encrypted communications of '351 because proper key management techniques can help protect key and data security.

11. Claim 5 rejected under 35 U.S.C. 103(a) as being unpatentable over '351 in view of "Security Service API" in further view of "An Introduction to Microsoft NetShow Services and Advanced Streaming Format" (hereafter referred to as IMNSASF).

As to claim 5:

12. '351 as modified above teaches a method for controlling access to data using the CryptoAPI on a user computer running Windows. '351 as modified above does not teach to determine if program code implementing cryptor, compressor and authenticator is stored on the first data processing apparatus, and if not, download the code from another processing apparatus. IMNSASF teaches an automatic download feature for downloading new codecs in a Windows environment (Page 3, Line 4, IMNSASF). It would have been obvious to a person of ordinary skill in the art at the time of invention to use the Windows automatic codec download feature taught in IMNSASF with the Windows CryptoAPI to download new encryption/decryption codecs. One of ordinary skill in the art would have been motivated to the Windows automatic codec download feature taught in IMNSASF with the Windows CryptoAPI to download new encryption/decryption codecs because this feature would provide a simpler easier interface for obtaining new encryption algorithms.

13. Claim 6 rejected under 35 U.S.C. 103(a) as being unpatentable over '351 in view of Yoshimune et al., US Patent No. 6438233 (hereafter referred to as '233).

As to claim 6:

14. '351 teaches a method for controlling access to data using determined attributes including encryption keys. '351 Does not teach transmitting program code implementing the decoding process as part of determined attributes. '233 teaches an encrypted data communication system where the deciphering algorithm is transmitted with the encryption key (Col 26, Line 55 et seq., '233). It would have been obvious to a person of ordinary skill in the art at the time of invention to use the algorithm/key transportation feature of '233 with the data encryption/communication system of '351. One of ordinary skill in the art would have been motivated to use the algorithm/key transportation feature of '233 with the data encryption/communication system of '351 because to do so would provide flexibility of expansion for using a new encryption algorithm.

15. Claims 8 and 13 rejected under 35 U.S.C. 103(a) as being unpatentable over '351 in view of "Customizing Logs and Reports" (hereafter referred to as CLR).

As to claims 8 and 13:

16. '351 teaches a method for controlling access to data using determined attributes including encryption keys transferred between servers. '351 does not teach to log the requests made for the determined attributes. CLR teaches creating server logs for each access request a server receives (Page 1, Line 19, CLR). It would have been obvious to a person of ordinary skill in the art at the time of invention to log the requests made for the determined attributes. One of ordinary skill in the art would have been motivated

to log the requests made for the determined attributes because it can later be used to analyze the requests a server receives helping with communications logistics.

17. Claims 9 and 14 rejected under 35 U.S.C. 103(a) as being unpatentable over '351 in view of Weiss et al., US Patent No 5237614 (hereafter referred to as '614).

As to claims 9 and 14:

18. '351 teaches a method for controlling access to data using encryption keys transmitted from a vendor to an access control device. '351 does not specifically teach to authenticate the user before generating/transmitting keys. '614 teaches a network security system for transmitting encrypted data first using an authentication procedure before key encryption and transmission. It would have been obvious to a person of ordinary skill in the art at the time of invention to use the authentication procedure before generating/transmitting encryption keys as in '614 with the access control system of '351. One of ordinary skill in the art would have been motivated to use the authentication procedure before generating/transmitting encryption keys as in '614 with the access control system of '351 because a personal authentication system would help guarantee that access rights are delivered to the proper individual.

Conclusion

19. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

20. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

21. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jonathan R Adams whose telephone number is (703) 305-8894. The examiner can normally be reached on Monday – Friday from 10am to 6pm.

22. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100